In the Claims

1. (Currently amended) A method of authentication, comprising the steps of:

a) sending first information from a contents-information receiver apparatus to a contents-information sender apparatus, the first information including a combination of certificate information representative of presence of a license granted to the contents-information receiver apparatus and ~~second~~ identification information for identifying the contents-information receiver apparatus, the first information further including a signal of a signature for the combination of the certificate information and the ~~second~~ identification information;

b) in the contents-information sender apparatus, determining whether the combination of the certificate information and the ~~second~~ identification information in the first information sent by the step a) is correct or wrong in response to the signal of the signature in the first information;

c) in the contents-information sender apparatus, extracting the ~~second~~ identification information from the first information sent by the step a) and storing the extracted ~~second~~ identification information;

d) sending the ~~second information for the contents-information receiver apparatus~~ identification information from the contents-information receiver apparatus to the contents-information sender apparatus at a time different from a time of the step a); and

e) in the contents-information sender apparatus, collating the ~~second~~ identification information sent by the step d) with the ~~second~~ identification information stored by the step c).

2. (Original) A method as recited in claim 1, wherein the certificate information contains information of a reliability of the contents-information receiver apparatus.

3. (Currently amended) A contents-information sender apparatus comprising:

first means for receiving first information from a contents-information receiver apparatus, the first information including a combination of certificate information representative of presence of a license granted to the contents-information receiver apparatus and ~~second~~ identification information for identifying the contents-information receiver apparatus, the first information further including a signal of a signature for the combination of the certificate information and the ~~second~~ identification information;

second means for determining whether the combination of the certificate information and the ~~second~~ identification information in the first information received by the first means is correct or wrong in response to the signal of the signature in the first information;

third means for extracting the ~~second~~ identification information from the first information received by the first means and storing the extracted ~~second~~ identification information;

fourth means for receiving the ~~second information for the contents-information receiver apparatus~~ identification information from the contents-information receiver apparatus at a time different from a time of receiving by the first means; and

fifth means for collating the ~~second~~ identification information received by the fourth means with the ~~second~~ identification information stored by the third means.

4. (Original) A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains information of a reliability of the contents-information receiver apparatus.

5. (Currently amended) A contents-information receiver apparatus comprising:

first means for sending first information to a contents-information sender apparatus, the first information including a combination of certificate information representative of presence of a license granted to the contents-information receiver apparatus and ~~second~~ identification information for identifying the contents-information

receiver apparatus, the first information further including a signal of a signature for the combination of the certificate information and the ~~second~~ identification information; and

second means for sending the ~~second information for the contents-information receiver apparatus~~ identification information to the contents-information sender apparatus at a time different from a time of sending by the first means.

6. (Original) A contents-information receiver apparatus as recited in claim 5, wherein the certificate information contains information of a reliability of the contents-information receiver apparatus.

7. (Currently amended) An authentication system including a contents-information sender apparatus and a contents-information receiver apparatus, the authentication system comprising:

first means for sending first information from the contents-information receiver apparatus to the contents-information sender apparatus, the first information including a combination of certificate information representative of presence of a license granted to the contents-information receiver apparatus and ~~second~~ identification information for identifying the contents-information receiver apparatus, the first information further including a signal of a signature for the combination of the certificate information and the ~~second~~ identification information;

second means provided in the contents-information sender apparatus for determining whether the combination of the certificate information and the ~~second~~ identification information in the first information sent by the first means is correct or wrong in response to the signal of the signature in the first information;

third means provided in the contents-information sender apparatus for extracting the ~~second~~ identification information from the first information sent by the first means and storing the extracted ~~second~~ identification information;

fourth means for sending the ~~second information for the contents-information receiver apparatus from the contents-information receiver apparatus~~ identification

information to the contents-information sender apparatus at a time different from a time of sending by the first means; and

fifth means provided in the ~~the~~ contents-information sender apparatus for collating the ~~second~~ identification information sent by the fourth means with the ~~second~~ identification information stored by the third means.

8. (Original) An authentication system as recited in claim 7, wherein the certificate information contains information of a reliability of the contents-information receiver apparatus.

9. (Currently amended) A method as recited in claim 1, wherein the certificate information contains a signal of a public key being a mate to a secret key for generating the signal of the signature from the combination of the certificate information and the ~~second~~ identification information.

10. (Original) A method as recited in claim 1, wherein the certificate information contains information related to a copyright on contents.

11. (Original) A method as recited in claim 1, wherein the certificate information contains public information given only to licensees.

12. (Original) A method as recited in claim 1, wherein the certificate information contains a signal of a public key peculiar to the 1 0 contents-information receiver apparatus.

13. (Original) A method as recited in claim 1, wherein the certificate information is given to the contents-information receiver apparatus by a management organ.

14. (Original) A method as recited in claim 1, further comprising the step of, after the step e), exchanging a signal of a first key and a signal of a second key between the

contents-information sender apparatus and the contents-information receiver apparatus.

15. (Currently amended) A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains a signal of a public key being a mate to a secret key for generating the signal of the signature from the combination of the certificate information and the ~~second~~ identification information.

16. (Original) A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains information related to a copyright on contents.

17. (Original) A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains public information given only to licensees.

18. (Original) A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains a signal of a public key peculiar to the contents-information receiver apparatus.

19. (Original) A contents-information sender apparatus as recited in claim 3, wherein the certificate information is given to the contents-information receiver apparatus by a management organ.

20. (Original) A contents-information sender apparatus as recited in claim 3, further comprising sixth means for, after the collating by the fifth means, exchanging a signal of a first key and a signal of a second key with the contents-information receiver apparatus.

21. (Currently amended) A contents-information receiver apparatus as recited in claim 5, wherein the certificate information contains a signal of a public key being a

mate to a secret key for generating the signal of the signature from the combination of the certificate information and the ~~second~~ identification information.

22. (Original) A contents-information receiver apparatus as recited in claim 5, wherein the certificate information contains information related to a copyright on contents.

23. (Original) A contents-information receiver apparatus as recited in claim 5, wherein the certificate information contains public information given only to licensees.

24. (Original) A contents-information receiver apparatus as recited in claim 5, wherein the certificate information contains a signal of a public key peculiar to the contents-information receiver apparatus.

25. (Original) A contents-information receiver apparatus as recited in claim 5, wherein the certificate information is given to the contents-information receiver apparatus by a management organ.

26. (Currently amended) A contents-information receiver apparatus as recited in claim 5, further comprising third means for exchanging a signal of a first key and a signal of a second key with the contents-information sender apparatus after ~~second-information~~ identification-information collation is done by the contents-information sender apparatus.

27. (Currently amended) An authentication system as recited in claim 7, wherein the certificate information contains a signal of a public key being a mate to a secret key for generating the signal of the signature from the combination of the certificate information and the ~~second~~ identification information.

28. (Original) An authentication system as recited in claim 7, wherein the certificate information contains information related to a copyright on contents.

29. (Original) An authentication system as recited in claim 7, wherein the certificate information contains public information given only to licensees.

30. (Original) An authentication system as recited in claim 7, wherein the certificate information contains a signal of a public key peculiar to the contents-information receiver apparatus.

31. (Original) An authentication system as recited in claim 7, wherein the certificate information is given to the contents-information receiver apparatus by a management organ.

32. (Original) An authentication system as recited in claim 7, further comprising sixth means for, after the collating by the fifth means, exchanging a signal of a first key and a signal of a second key between the contents-information sender apparatus and the contents-information receiver apparatus.